UNIVERSITY OF BIRMINGHAM

Information Security

User Guide

Contents

What is Information Security and Who Does it Concern? 3
Policies 4
Information Classification 5
Common Criteria 6
Data Protection 7
Threats 8
Social Engineering 8
Phishing 9
Common Cyber Attacks 11
Advanced Persistent Threats 12
Controls 14
Authentication 14
Passwords 15
Secure Email 17
Email Best Practice 18
Remote Access 18
Payment Card Information 19
Mobile Security 19
Portable Media – USB sticks, DVDs etc. 20
Data Storage 22
Cloud Storage 22
Hard Copies / Paper Documents and Fax 23
Security Awareness Training 23

What is Information Security and Who Does it Concern?

The University operates in a highly competitive environment where the ability to manage and protect information is critical. Effective security is needed to comply with the law, fulfil contractual obligations and is key to attracting research funding.

'Information Security' refers to the concepts and activities associated with protecting important qualities or properties of information, including:

- **Confidentiality** – protecting against unwanted access to information,
- **Integrity** – preventing unwanted changes to information,
- **Availability** – delivering information where and when needed,
- **Dependability** – ensuring consistency and predictability,
- **Accountability** – tracking user and system actions.

These properties can be thought of as the legitimate concerns of stakeholders in the University's information resources:

Information Asset Owners	The *Business Owners* of the information, who are accountable to the University for assets.
Information Security Risk Owners	Defined roles include: • Senior Information Risk Owner (SIRO), • Data Protection Officer, • Caldicott Guardian (medical records only), • Information Security Officer.
University Senior Officers	Executives and senior managers responsible for setting overall policy goals and defining the University's tolerance of risk.
Members	All members of the University including staff and students.
Public	The general public.

You may not feel concerned about security because you do not often come across or have to deal with anything confidential. Beware, this is a false

impression. You are still a target of attacks such as phishing or social engineering that seek to gain any toehold that could be used in later attacks.

At some point, probably without warning, you will inevitably have access to someone's personal information. If you are found to be responsible for a breach you may be subject to a fine from the Information Commissioner and probably some sort of disciplinary action by the University. This can happen even if the incident was an accident, theft or as a consequence of someone else's action.

To protect yourself you need to be know the rules, follow them and be seen to be following them.

Information Security is everyone's concern and everyone's problem.

Policies

Information Security at the University is governed by the Information Security Policy (ISP) and related standards documents that expand on particular sections of the policy. Policies, standards and guidance documents can be accessed on the University intranet web site at www.it.bham.ac.uk/policy.

There is also an overarching University Code of Practice, the 'General Conditions of Use of Computing and Network Facilities' that sets out the basic rules concerning access to the University's information and computing resources.

Compliance depends on the type of document:

- **Code of Practice** – Mandatory, the General Conditions of Use is signed by all and forms part of a member's contract with the University.
- **Policies** – Mandatory for staff and students.
- **Standards** – Expected, exceptions must be justified.
- **Procedures and Guidelines** – advisory only.

To reinforce accountability, you will receive email notifications from the Policy Affirmation System (PAS) asking you to acknowledge a list of policies, not just the ISP but others relevant to your role.

Information Classification

The physical and electronic containers of information are known as *information assets* because they have a quantifiable value to the University, like other assets. Assets may be tangible such as computers, disks, networks, files, database, documents and email messages or intangible – reputation, goodwill etc. Tangible assets may be harmed directly while intangible assets usually suffer harm as a consequence of attacks on other assets, people or processes.

The University has introduced an Information Classification Scheme that provides a framework for identifying and classifying information assets according to the impact of a breach in confidentiality. The scheme is based on three categories:

Confidential

Likely to cause *significant* harm to the University's reputation, assets or ability to meet legal or contractual obligations if revealed outside intended audience.

Restricted

Intended for a defined audience but not particularly sensitive.

Open

Intended for the public domain and carries no appreciable confidentiality risk.

Data classification may vary throughout the life-cycle of an asset. Some assets may start their life as Confidential but have their classification reduced upon publication or when they are superseded by a new version.

Everyone must ensure that any asset containing Confidential information is marked and handled accordingly.

The business owners of information, known as 'Information Asset Owners' (IAO), have responsibility for deciding on the appropriate classification based on risk assessments.

All users must ensure that the files, documents, databases and devices they handle are marked with the appropriate category.

Common Criteria

The following examples are based on agreed guidelines proposed by users across the University.

Personal	Personnel files held by Human Resources, or Colleges, Schools and Departments. CVs, job applications, interview results, candidate assessments and personal details.	**Confidential**
	Student or staff welfare or disciplinary cases.	**Confidential**
	Personal photographs, sensitive personal data.	**Confidential** except by consent
Academic	Live examination papers	**Confidential**
	Past examination papers	**Open**
	Student assessments	**Confidential**
	Unpublished research papers	**Restricted** or **Confidential**
	Published research papers	**Open**
	Research funding applications	**Restricted**
	Patient identifiable data, medical records	**Confidential**
Commercial	'Commercial in Confidence', contracts, tenders for contracts	**Confidential**
Committees	Council, UEB minutes and papers	**Confidential**
	Other minutes and papers	**Restricted**
Internet	Public web sites, *outer* intranet	**Open**

Note that these are examples for guidance only and it is expected that the list will grow and change over time as we gain experience.

Data Protection

The Data Protection Act 1998 applies to all records containing personal information which identify living Individuals and includes manual (paper) records, CCTV tape, photographs and audio tapes as well as computer held data. The DPA governs the collection, storage, use and disposal of personal information and lays down 8 principles that must be followed.

Personal information must:

1. Be processed fairly and lawfully.
2. Be collected for a specific purpose.
3. Not be excessive.
4. Be accurate.
5. Not be kept longer than necessary.
6. Be handled in line with the subject's rights.
7. Be protected and kept securely.
8. Be protected if sent overseas.

Personal information includes:

Name, address, telephone number, email address, date of birth, National Insurance Number, HR records, academic records, bank account details etc.

This must be treated as confidential unless disclosed with consent, or by virtue of a contract or in accordance with the act. Additionally, *sensitive* personal data must always be treated as Confidential except with the explicit consent of the individual concerned:

Race or ethnic origin, political or religious convictions or similar beliefs, trade union membership, physical and mental health, sexual orientation and activity, and criminal allegations, proceedings or convictions.

In practice all personal data, including CVs and academic records such should be classified as Confidential and should always be dealt with in accordance with the 8 Data Protection Principles.

For more information, contact the Information Compliance Manager via email on legalservices@contacts.bham.ac.uk and refer to the Data Protection Policy at www.legalservices.bham.ac.uk/dppolicy. Further general guidance can be found on the Information Commissioner's website http://www.ico.gov.uk.

Breaches of the Data Protection Act must be reported immediately to the University's Data Protection Officer Carolyn Pike, Director of Legal Services by calling 0121 414 3916.

Threats

The University is continually scanned by attackers looking for potential vulnerabilities – **'Cyber Warfare'** is not too strong a term to use. Among the most important threats facing the University are:

1. Loss of valuable intellectual property to specialised or sophisticated attackers with high capability. The University is a high profile target for criminal and state-sponsored groups motivated by financial gain or national competitiveness. In some cases, criminal organisations are paid by foreign states to steal intellectual property.
2. Loss of personal details of staff and students that breaches the Data Protection Act. This is often casual or accidental, except where part of a larger, coordinated attack.
3. Loss of patient identifiable data obtained for clinical trials and other research activities, from the NHS. The University is registered with the NHS Information Guidance scheme as a 'secondary uses organisation' and is contractually obliged to comply with their requirements. There is a similar situation with data from the pupil information database of the Department for Education

Social Engineering

In the context of Information Security, the term 'Social Engineering' is used to describe attacks aimed at people. It can take many forms but is usually aimed at exploiting weaknesses triggered by the occasional lack of awareness of University staff and students. This document is part of a communications initiative aimed at mitigating the risk of such attacks by providing you with essential background knowledge.

Social engineering attacks may be targeted at individuals who play a role in assigning or managing user accounts. Attackers often pose as authority figures and seek to impose their will or take advantage of the goodwill or helpfulness of staff.

Baiting

A type of social engineering attack, where portable media, such as a USB flash drive, containing malware is deliberately left where it is likely to be found. Sometimes these have a logo, or keys attached, that helps to make them

look more legitimate and encourages the victim to plug in to a computer in order to find the owner.

Beware of 'freebie' or promotional USB sticks as these are often pre-loaded with malware waiting to trap the unwary.

Whaling

Cyber-attacks targeted specifically at senior officers and other high profile targets. Again, these can be very convincing and are often based on quite detailed research.

Examples

Some typical attack scenarios are:

- a caller poses as a senior member of the University and tries to persuade a member of staff to reset their password directly over the telephone, bypassing the normal procedures.
- a request for information expressed in vague terms such as 'send me this year's figures' using a plausible but false identity.
- email 'phishing' attacks where an email message from a plausible email address requests the user to go to an external web site and input their password or other credentials.

What to Do

All of us need to be vigilant in detecting and resisting such attacks. Even if you believe that you don't have access to anything remotely confidential, you may still be targeted. An attacker will seek to gain any kind of legitimate access as a stepping stone to further mischief.

You need to keep yourself up to date with the Information Security Policy and stay vigilant. This booklet and the online Information Security Awareness Training should help.

Phishing

The term used for attacks that use of email to lure people into disclosing their passwords, or other credentials, with the result that the user account is compromised and the attackers gain access to the University's information.

Typical attacks take the form of an unsolicited email

message from a respectable-looking address that asks you to click on a link that takes you to a web page where you are asked to input your user identifier and password. If you do this, you will have compromised your account and the attacker is free to use your University account. Some of the more genuine-looking phishing attacks use internal email accounts that have been compromised, allowing attackers access to the University's systems or information by impersonating legitimate users.

Some phishing emails are very obvious but others are more convincing because they reuse information gleaned from earlier attempts.

Short URLs

It has become common to receive emails with 'short' hyperlinks that refer back to an external service such as bitly.com. The short link is replaced by the actual URL by the external service and there is no control or visibility of where the link goes or what is waiting at the other end.

Avoid clicking on these short hyperlinks unless you know the sender and are confident the email is genuine.

Spear Phishing

Phishing attacks targeted at a specific individual or a small number of people are known as 'Spear Phishing'. These can be very convincing because they are often based on detailed research and may be part of an advanced threat involving a series of steps spaced out over time.

If you are a member of a team that has access to valuable intellectual property, you may be targeted in this way. Even if you don't personally have access to anything confidential, you could be used as a stepping stone to gain a foothold that can be subsequently used to leverage requests for greater privileges.

What to Do

The only way to be safe is to ignore any **unsolicited** email with a link that sends you to an external (Internet) site where you are asked to input your user identifier and password (or even just the password since the user identifier can be discovered in other ways). Any emails purporting to be from 'system administrators', 'IT Services' or similar that lead you to a web page where you are expected to input your password are suspect. Note that it is very easy to create a convincing looking email or web site by copying University graphics and duplicating the look and feel.

Hover over the link with the mouse and take a look at the URL displayed. If it resembles or starts with:

- http:// if it doesn't start with 'https://' (indicating SSL security) then, phishing or not, it's insecure and you should not input your credentials under any circumstances.
- https://123. a numeric value with embedded dots (IP address) means it's likely to be an attack; the University does not use bare IP addresses in hyperlinks.
- https://xxxxxx.birmingham.ac.uk or https://xxxxxx.bham.ac.uk where xxxxxxx is something meaningful and recognisable such as 'intranet', 'canvas', 'policyaffirmations', 'www' or 'findit' is probably safe and you can sign-on if prompted.

There are also some legitimate University web sites where you will be expected to sign-on with your University credentials such as the IT Service Desk (https://www.universityofbirmingham.service-now.com) and Canvas (https://www.birmingham.instructure.com). These are perfectly safe to use.

Be aware that if your browser is not set up correctly for single sign on (SSO), you may be prompted to sign on when accessing an internal site such as the intranet, Sharepoint team sites or web applications. Linux and Mac users may be particularly affected by this.

If in doubt, ask your line manager or IT Support team before potentially compromising your password.

You will receive fake emails, just ignore and delete them. There's generally no need to inform IT Services as they arrive daily by the thousand!.

Common Cyber Attacks

Denial of Service

Denial of Service attacks involve flooding a target with a high volume of messages so that it is overwhelmed and ceases to function correctly or respond to legitimate requests. Often these attacks make use of 'bots' or computers that are connected to the Internet and have been 'seeded' by malware that participate in the attack, responding to commands sent by the instigators - this type is known as **Distributed Denial of Service** (DDoS**)**. The participating

bots are often home computers infected with malware that participate unwittingly. Sometimes many thousands of them may take part in an attack.

Denial of service attacks are usually countered using firewalls – networking equipment that filters unwanted types of message traffic.

Injection

Injection flaws, such as SQL, XML, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data. Injection attacks are possible because of software architectures that include the use of command-line or code interpreters as opposed to application programming interfaces (APIs).

Cross-site Scripting (XSS)

These flaws occur when an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

URL Hacking

Many web applications add parameter values to URLs as a way of preserving them between web pages. But attackers can edit the URL string, substituting their own values that may be used to trick an application into returning unauthorised data or making uncontrolled changes.

Advanced Persistent Threats

Advanced Persistent Threats (APTs) use multiple avenues of attack and often take a 'thin end of the wedge' approach that starts with minor incursions and builds over time. They can be very difficult to detect and may evade traditional security measures such as firewalls and intrusion detection software. The terminology is derived from their characteristics as follows:

- **Advanced** – The attackers are expert in cyber-intrusion methods and are capable of crafting custom exploits and tools.
- **Persistent** – Attackers have long-term objectives and will persistently work to achieve them without regard for time.
- **Threat** – Attackers are organised, funded, well trained and motivated.

APTs can be highly damaging, often provoking a 'ripple effect' that spreads across an entire industry or national infrastructure.

They tend to have a consistent life cycle:

1. Initial intrusion by exploiting system vulnerabilities or social engineering.
2. Malware is installed on compromised systems.
3. Outbound communication is initiated
4. Attacker spreads laterally to adjacent systems
5. Compromised data is extracted.
6. Attackers cover their tracks.

Attacks can be very difficult to detect after they are complete, so it is important to try to detect and deal with them while they are still under way.

Controls

Authentication

This is about verifying users' identities as they access the system. For most, it takes the form of signing-on at a computer, tablet or smartphone - usually involving just one 'authentication factor'- a password typed into a sign-on screen.

Authentication Factors

There are three factors that may be used to verify a user:

- **Something you know** – such as a password, pass-phrase or PIN.
- **Something you have** – a 'token' such as an RSA fob, that generates a unique code, a smartcard with a coded certificate or similar.
- **Something you are** – biometric data that can be verified using a reader – a voiceprint, fingerprint etc.

More factors usually means better security. User names and email addresses are not authentication factors because they are widely known or easily guessable.

Single-factor authentication is the most common and is used on-campus, usually with a password (or sometimes a smartcard).

2-factor authentication is used for remote access to University core business applications and information resources via the Internet. The University will provide this access to all staff who need to work from home or while travelling by using a 'soft token' consisting of a mobile app that generates a one-time numeric code or a 'hard token' or fob that does the same.

3-factor authentication may be used in the future for special situations such as highly confidential research projects.

Single Sign-On (SSO)

Single sign-on is where the user is authenticated once and then the system remembers them so they do not have to keep signing-on as they navigate between applications and information resources.

This is best done by passing around an encrypted token or certificate that cannot be falsified and proves the user's identity. When the user signs-off, or

after a defined timeout period (e.g. 15 minutes), the token is deleted forcing the user to re-authenticate.

SSO is considered more secure because it can be reinforced without having to change a multitude of individual applications.

Passwords

Passwords are the most common authentication factor and the rules governing their use are defined in the University's Access Management Standard.

Follow the golden rules

1. Maintain a different strong password for each system or service that requires one.
2. Do not divulge your passwords to anyone.
3. Keep passwords safely and securely.

User accounts are usually suspended after five consecutive unsuccessful sign-on attempts. If this happens you will need to contact the IT Service Desk to have the password reset.

The strength of a password is a measure of its resistance to being guessed and is therefore a function of length, complexity, and randomness. As general guidance, consider the following:

- The longer, the better.
- A mixture of any of:
  - Lowercase (a-z)
  - Uppercase (A-Z)
  - Numbers (0-9)
  - Non-alphanumeric (e.g. [} ! # or %)
- Something not easily linked to you
- Something memorable.

The best passwords mean something to you but not to anyone else.

Bad Examples

- Your username with a number on the end and/or reversed.
- A partner's or relative's name.

- Words found in a dictionary, even a specialist dictionary such as literary figures, geological terms, foreign words, etc.
- Common character sequences (such as qwertyu).

Good Examples

- Phrase-based mnemonics "KmeKyou..bIcdooo!" (Knowing me knowing you .. best I can do).
- Random, multi-word phrases "Horse[Staple]fly munch".

Your password is your personal responsibility. It is the key to accessing information under your control and you are accountable for its misuse.

How Hackers Get Your Password

There are five common techniques that hackers use to obtain your password:

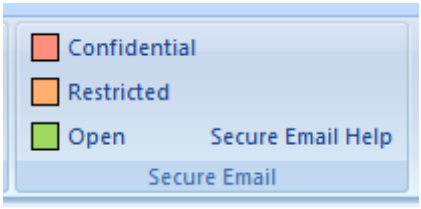
1. **Grab it** – looking over your shoulder as you type it ("shoulder-surfing") or finding the piece of paper where you wrote it down. This is the most common way that passwords are compromised. If you do write your password down, you must keep the piece of paper safe. Avoid typing in your password if someone is watching.
2. **Steal it** – surfing dubious sites, or even legitimate ones that have been compromised by cybercriminals, can infect your machine with keyloggers, trojans and other forms of malware, which will silently capture and siphon off your personal data. Ensure your antivirus software is up-to-date and that you navigate the internet carefully and don't use your main University password anywhere else on the web.
3. **Guess it** – it's amazing how many people use a password based on information that can easily be guessed. Psychologists say that most men use four-letter obscenities as passwords and most women use the names of their boyfriend, husband or children.
4. **Brute force attack** – where every possible combination of letters, numbers and symbols is tried in an attempt to guess the password. While very onerous, with modern computing power and sophisticated software tools, it is now feasible to crack an eight-character random password in less than 2 hours while a fourteen-character password is still well out of reach.

5. **Dictionary attack** – a more intelligent method than the brute force attack is the dictionary attack. The combinations tried are first chosen from words available in a dictionary. Software tools are readily available that can try every word in a list until your password is found.

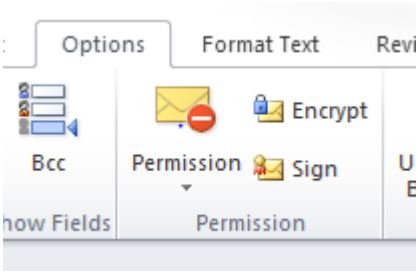
There may be occasions where a password **must** be given to an authorised individual or body, such as a technician attempting to replicate a problem, to the police or other law enforcement agency or authority, or to Customs officials at an international border. In these cases, you must change the password at the earliest opportunity afterwards.

Secure Email

The University provides a secure email facility with the central University email account. An Outlook plug-in automates the *encrypt* and *sign* buttons, allowing the user to classify an email appropriately and then leave it to the system to take appropriate action.



Those who do not have the Traffic Lights plug-in, or use another email client program, should use the *encrypt* and *sign* buttons or their equivalent directly. In Outlook, these buttons are found on the *message options* tab.



The *sign* button attaches a digital signature to the message, thus proving its integrity. An exchange of signed emails is the main method used to set up email encryption arrangements with people outside the University.

Email Best Practice

When using email:

1. Encrypt email messages, using the Outlook traffic lights or encrypt button (or equivalent in other email client programs) containing Confidential information or with Confidential attachments.
2. Sign messages, using the sign button in Outlook or equivalent in other email client programs, to protect against tampering or when setting-up mutual email encryption with someone outside the University.
3. Avoid using email for Confidential information if you cannot use encryption with a given correspondent, or remove or minimise the sensitive content.
4. Do not forward, redirect or otherwise cause Confidential email or attachments to be stored in insecure public email. Some well-known service providers, including Google and Yahoo, have suffered serious security breaches and just do not meet our security requirements.
5. Avoid storing University email on smartphones or tablets except using approved mobile device management (MDM) software 'Good for Enterprise' or an alternative that has been formally approved by IT Services.
6. All users may freely access University email using Outlook Web Access (OWA) from any public or private computer or device because it does not store messages on the user device.

Do not encrypt email that is not confidential – as this prevents scanning for malware and other security measures.

Remote Access

Those members of the University who wish to access the University's core systems, or Confidential information, from off-campus locations need to have been authorized by their line manager.

The University offers a secure Virtual Private Networking (VPN) facility. You will need to sign-on using your University Single Sign On user identifier

and password, and input a one-time code generated by a security key fob or sent to a mobile phone application that IT Services will provide.

You will need to request access via the IT Service Desk. If requesting access to University core business system, or an information resource containing confidential data, the Information Asset Owner (IAO) will need to approve the request.

The level of access provided each time you connect may vary according to your geographical location and the type of device being used. This means that you may be given more restricted access when connecting from a public computer, or from certain parts of the world.

Payment Card Information

If your work involves contact with credit or debit card information, such as the card number, expiry date or security code, then how you handle that information must comply with the Payment Card Industry Data Security Standard (PCI DSS). Compliance reduces the risk of card data theft and fraud and so helps ensure a secure environment for university customers to make payment. The University, like all other merchants, is contractually obliged to comply with the standard as a condition for accepting card payments.

What you need to do to comply varies according to exactly how you handle card information. Guidance is available at:
intranet.birmingham.ac.uk/PCIDSS.

For more information email pcidss@contacts.bham.ac.uk.

Mobile Security

Because of their size and portability, mobile devices such as smartphones and tablets, can provide a major boost to productivity – but they have a significant vulnerability when it comes to storing confidential critical information.

Ideally, confidential information should not be stored on these devices at all. However if this cannot be avoided then the following rules apply:

1. **Copy** – the data stored on the mobile device must be a copy only. The original or master copy should kept safe in the University's central data stores.

2. **Strong password –** access to the device should require reliable authentication of the user with a strong password as defined in the Access Management Standard. A four digit device unlock code is not considered sufficient protection by itself.
3. **Timeout –** the device's screen should be set to lock after a period of inactivity no longer than 60 seconds.
4. **Encryption –** full disk or file-level encryption to a level that conforms to the University's Cryptography Standard. Encryption is pointless however, unless it is accompanied by a strong password or equivalent.

Mechanisms

The following security mechanisms satisfy the mobile security requirements:

- **Mobile Device Management (MDM)** – the University has selected '**Good for Enterprise** MDM software for email only.
- **Blackberry** – provides MDM based on the 'Good for Enterprise' software for email only.
- **Boxcryptor** – protects data stored on mobile devices and cloud storage services such as **Dropbox**, **Skydrive** etc.
- **Bitlocker** – encryption for Windows-based smartphones and tablets.

Other measures will be added to the approved list from time to time.

Portable Media – USB sticks, DVDs etc.

Confidential information should never be stored on portable media unless it is adequately protected. Portable media includes:

- DVDs and other types of rewriteable disk.
- USB flash memory sticks.
- magnetic tape cartridges.
- portable hard disk drives.
- smartphones used as portable disk drives.

It's best to avoid storing anything Confidential on them at all, but if it cannot be avoided then you should ensure that the data is encrypted, is clearly marked

and stored in a locked cupboard or drawer when not in use. You should avoid carrying around portable media containing Confidential information where possible.

Encryption

The following encryption software is approved for use with portable media:

- **Bitlocker** – encryption provided with Windows. Windows users can encrypt a USB stick, DVD or anything that can be represented as a disk available by right-clicking in Windows 7 onwards.
- **Truecrypt** – freeware encryption software.
- **Boxcryptor** – commercial encryption software that provides multi-platform support including PCs, tablets and smartphones.

DVDs

Confidential data must be encrypted on all portable disks, including DVDs. Windows users can encrypt using Bitlocker and others can use Truecrypt.

USB Flash Memory

The USB stick should be encrypted in accordance with the University's Information Security Policy (ISP) and Cryptography Standard. The highest level of security is provided by hardware encrypted USB sticks, although software encryption can be almost as good (and considerably cheaper).

Backup Tape Cartridges

Confidential data must not be backed-up to tape unless it is properly encrypted. This usually means that the confidential files must be stored encrypted or encrypted before the backup software is run. If a backup tape contains any confidential data, it must be clearly labelled and kept in a locked cabinet.

Portable Hard Disk Drives

Again, portable hard drives should be treated like other portable media. If Confidential information is to be stored on them, it should be encrypted and the drive clearly labelled and stored in a locked cabinet when not in use. Do not leave it on your desk overnight or when absent.

Smartphones

Modern smartphones often have a considerable amount of storage that can be used as a portable file store. This can be very useful but you should still ensure that all Confidential data is properly encrypted as with other portable media. The built-in disk encryption should be used (provided that access is controlled using a strong password), or a product such as Boxcryptor. If a smartphone or tablet is used to access cloud storage services, you must ensure that any Confidential data is encrypted.

Printing

Care must be taken when printing Confidential documents. They must not be sent to an unattended remote printer or left on a printer where anyone passing might read or take the document away. Use 'follow me' printing or ensure that a trusted person is standing by the printer to receive the document.

Data Storage

Confidential data **must** be stored encrypted, except where it is safely inside a protected network zone such as the campus data centre network. The encryption **must** be done using a product that complies with the Cryptography Standard. You should follow the following rules:

1. Encrypt **Confidential** data except when stored in a central University data store in a secure network zone and not directly accessible from user devices inside or outside University networks.
2. Do not encrypt **Restricted** or **Open** data so that it can be scanned for viruses and other malware.
3. Avoid storing **Confidential** data on laptops, desktops, mobile devices and removable media else ensure it is encrypted and protected by a strong password.

Cloud Storage

1. Encrypt Confidential data using a product that conforms to the University Cryptography Standard, such as:
    - **Truecrypt** – freeware encryption software.
    - **Boxcryptor** – commercial encryption software that provides multi-platform support including PCs, tablets and smartphones.

2. Ensure physical storage is within UK or EEA or the supplier is Safe Harbour certified.

Cloud storage services such as DropBox or SkyDrive should not be used for confidential files unless they are encrypted using an approved product such as BoxCryptor.

Hard Copies / Paper Documents and Fax

1. If **Confidential**, mark on every page.
2. If **Restricted**, mark at least on the front page or exterior cover.
3. Store **Confidential** papers in a locked cabinet with known key holders. Do not leave them lying around on printers where anyone can see them.
4. Do not fax **Confidential** information unless a trusted person is standing by at the other end to receive it.

Destruction

1. If **Confidential**, shred paper copies (preferably cross-cut) or use the University's secure disposal service.
2. Delete **Confidential** files and overwrite removable media using an approved utility.

Security Awareness Training

Online training is available via the Canvas Virtual Learning Environment. This is mandatory for all staff and some students, a requirement imposed by external partners such as the NHS, and should be repeated annually. To access the course go to intranet.birmingham.ac.uk/it/security/training.